REMARKS

In the Final Office Action dated March 21, 2007, claims 1-3, 5-8, 10-13, 15-18, 20-23 and 25 were rejected under 35 USC 103 as being unpatentable over the combination of Rosner (U.S. Patent 6,636,968), Kato (6,381,331) and Schneier ("Applied Cryptography"). To simplify the issues remaining, and to expedite the prosecution of this application to its successful conclusion, claims 1, 2, 5-7, 10-12, 15-17, 20-22 and 25 are canceled herein, Claims 3, 8, 13, 18 and 23 remain as the only independent claims. New claims 26-29, dependent from claims 3, 8, 18 and 23 are added. It is respectfully submitted that the claims present in this application are patentably distinct over this combination for the reasons now discussed.

All the claims present in this application recite the feature that is best found in claim 3 as follows:

> generating on the basis of said encryption key, a set of passkeys specific to each of said specific destinations by dividing said encryption key by a division pattern unique to each of said specific destinations and said division pattern based on the content of said digital data;
>
> generating a plurality of partial keys based on a portion of the passkeys in said set or a portion of passkey information from which said passkeys may be reproduced;
>
> delivering either said plurality of partial keys or partial key information, from which said partial keys may be reproduced, and delivering the remaining passkeys not used to generate said partial keys or the remaining passkey information, to each of said specific destinations over a plurality of delivery routes which differ from routes for delivering said digital data and which are further different from each other ...

It is respectfully submitted, the combination of references relied upon in the Final Rejection of March 21, 2007 fails to suggest the limitations quoted above. Rosner, col. 3, lines 40-60, was relied upon by the Examiner as a teaching of these limitations. However, this portion of Rosner states that a "session key" is based upon a secret key and public keys from destination

devices. Rosner also mentions that partial keys are generated by the key generator 220; and these partial keys are created such that "a knowledge of the private key ... of each corresponding destination device ... and a knowledge of a common group key ... facilitates a determination of a decryption key ... that is suitable for decrypting the encrypted content material." But, there is no description in Rosner or in Kato or Schneier of generating a **set** of passkeys specific to each destination, on the basis of the encryption key, and generating a plurality of **partial keys based on a portion of the passkeys (or a portion of the passkey information)**, as recited in all of Applicants' claims.

Applicants continue to argue that the feature of "dividing said encryption key by a division pattern unique to each of said specific destinations and said division pattern based on the content of said digital data" is not found in Schneier or in Rosner or Kato, notwithstanding the Examiner's comments in the Advisory Action mailed August 30, 2007. Section 3.6 (Secret Splitting) of Schneier divides a **message** into pieces by exclusive or-ing the message with two, three or more random-bit strings R, S, T, U, ... The result of this exclusive or operation is an encrypted message. There is no use of an encryption key to encrypt the message because there is no need to do so. Thus, there is no splitting of an encryption key using random numbers, as suggested by the Examiner. Not only is there no "key" to be split, but Schneier specifically states, in his last sentence of section 3.6, "Remember, M isn't being split in the normal sense of the word; it is being XORed with random values." It is respectfully submitted, the Examiner's interpretation of this description of Schneier as teaching one of ordinary skill in the art to divide keys is, at best, a strained interpretation not suggested by the clear understanding of Schneier. Moreover, the Examiner's conclusion that Schneier's statement that "M isn't being split in the normal sense of the word" is irrelevant is misplaced. Schneier's message is not an encryption

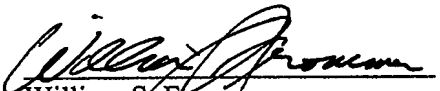
key. But, even if one attempted to construe Schneier's "message" as corresponding to Applicants' encryption key, Schneier teaches away from splitting the message (or encryption key) into a set of passkeys that, in turn, are used to generate plural partial keys. Accordingly, one of ordinary skill in the art, after reading and understanding Schneier and recognizing that an input message, or digital data, can be encrypted by XORing that digital data with a number of random-bit strings, would not be enabled thereby to generate a set of passkeys by dividing an encryption key by a unique division pattern. There simply is no suggestion in Schneier to divide or split anything, much less an encryption key. See the last sentence of Schneier's section 3.6, which clearly teaches away from "dividing said encryption key by a [unique] division pattern."

Claims 3, 8, 13, 18, 23 and 26-29 are in condition for allowance. An early notice to that effect is respectfully urged.

Please charge any additional fees that may be needed, and credit any overpayment to our Deposit Account No. 50-0320.

Respectfully submitted,

FROMMER LAWRENCE & HAUG LLP
Attorneys for Applicants

By: 
William S. Frommer
Reg. No. 25,506
(212) 588-0800